B. M. S. INSTITUTE OF TECHNOLOGY AND MANAGEMENT
YELAHANKA, BANGALORE-064
Department of Computer Science & Engineering

COURSE FILE CONTENTS

1. Calendar of Events
2. Time Table
3. Syllabus
4. Lesson Plan
5. Course Outcomes
6. CO – PO /PSO Mapping
7. Gap Analysis, Student activity plan & Articulation
8. List of Students
9. Internal Test Papers
10. Scheme of Evaluation
11. CO – PO Analysis-Excel sheet
12. Articulation for unattained PO`s
13. Three blue books,copy of assignment/Poster/PBL/reports etc

BMS INSTITUTE OF TECHNOLOGY AND MANAGEMENT

Avalahalli, Doddaballapur Road, Yelahanka, Bangalore - 560064

Department of Computer Science and Engineering

Calender of Events (CoE) 2020-21 (ODD Semester)

VISION OF THE INSTITUTE — To develop technical professionals acquainted with recent trends and technologies of computer science to serve as valuable resource for the nation/society.

MISSION OF THE INSTITUTE — Facilitating and exposing the students to various learning opportunities through dedicated academic teaching, g

Month	Week	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Working Days	EVENTS
September	W-1			1	2	3	4	5	5	1-Sept.: Commencement of B.E (III, V, & VII Sem.), MCA (III & V Sem.) & M.Tech (III Sem.) Classes; 1- Sept: Orientation for 3rd Sem Students; 2- Sept: PAC Meeting 1
	W-2	6	7	8	9	10	11	12	6	10-Sept.: FYP/PBL Group Formation; 10- Sept: Webinar on " Data Science"- IEEE
	W-3	13	14	15	16	17	18	19	5	17-Sept.: Mahalaya Amavasya; 18- Sept: Webinar on "Aerial Humanoid Robots"- IEEE; 19-Sept: Invited Talk by Industry Expert/Alumni -1
	W-4	20	21	22	23	24	25	26	6	21-Sept.: FYP/PBL Guide Allotment; 21 -Sept.: FIMS Update; 26 & 27- Sept: Workshop on Game Development -IEEE; 26-Sept: DAB Meeting
	W-5	27	28	29	30				3	30-Sept.: FYP/PBL Synopsis Submission
October	W-6					1	2	3	2	2-Oct.: Gandhi Jayanthi; 1- Oct: Test 1 Question Paper Scrutiny
	W-7	4	5	6	7	8	9	10	6	3-7 Oct.: Internal Assessment (IA) Test - 1 B.E (III, V, & VII Sem.) M.Tech (III Sem.), MCA (III & V Sem.); 9-Oct: Industry Interaction - 1
	W-8	11	12	13	14	15	16	17	6	14-Oct.: SMS Dispatch for IA-1 Academic Monitoring 1; 16-17 Oct.: Students Feedback -1 on Faculty; 17-Oct.: PTA for Higher Semester
	W-9	18	19	20	21	22	23	24	6	20-Oct.: FIMS Update; 23 Oct: Workshop on Simulator -CSI; 24-Oct: Invited Talk by Industry Expert/Alumni -2
	W-10	25	26	27	28	29	30	31	3	26-Oct.: Vijayadashami; 27-28 Oct.: FYP/PBL Patentability Review - 1; 30-Oct.: Eid Milad; 31-Oct.: Valmiki Jayanthi
November	W-11	1	2	3	4	5	6	7	6	1-Nov.: Kannada Rajyotsava; 2- Nov: Test 2 Question Paper Scrutiny; 3-7 Nov.:Internal Assessment (IA) Test - 2 B.E (III, V, & VII Sem.) M.Tech (III Sem.), MCA (III & V Sem.)
	W-12	8	9	10	11	12	13	14	6	14-Nov.: Tech-Transform 2020 Notification; 14-Nov.: SMS Dispatch for IA-2 Academic Monitoring 2; 13-Nov: Industry Interaction - 2
	W-13	15	16	17	18	19	20	21	5	16-Nov.: Balipadyami Deepavali; 16-17 Nov.: Students Feedback - 2 on Faculty; 20-Nov.: PBL Patentability Review - 2/BMSIT Open Day; 20-Nov.: FIMS Update; 21-Nov.: Tech-Transfrom 2020
	W-14	22	23	24	25	26	27	28	6	27-28 Nov.: FYP Patentability Review - 2
	W-15	29	30						1	
December	W-16			1	2	3	4	5	4	3-Dec.: Kanakadasa Jayanti; 4- Dec: Test 3 Question Paper Scrutiny
	W-17	6	7	8	9	10	11	12	6	7-9 Dec.: Internal Assessment (IA) Test -3 B.E (III, V, & VII Sem.) M.Tech (III Sem.), MCA (III & V Sem.); 12-Dec: Invited Talk by Industry Expert/Alumni -3
	W-18	13	14	15	16	17	18	19	4	16-Dec.: SMS Dispatch for IA-3 Academic Monitoring 3; 17-Dec.: Last Working Day for B.E (3rd, 5th, & 7th Sem.), MCA (3rd & 5th Sem.) & M.Tech (3rd Sem.) Classes
	W-19	20	21	22	23	24	25	26		21-Dec.: FIMS Update; 25-Dec.: Christmas; 26-Dec: PAC Meeting-2
	W-20	27	28	29	30	31				
	Total Number of Working Days								86	

CONTINUOUS INTERNAL EVALUATION

COURSE	SEM	START	END
INTERNAL ASSESSMENT - 1			
B.E	I	TBA	TBA
B.E	III, V, VII	05-Oct	07-Oct
MCA	III & V	05-Oct	07-Oct
M.Tech	I	TBA	TBA
MCA	I	TBA	TBA
INTERNAL ASSESSMENT - 2			
B.E	I	TBA	TBA
B.E	III, V, VII	05-Nov	07-Nov
MCA	III & V	05-Nov	07-Nov
M.Tech	I	TBA	TBA
MCA	I	TBA	TBA
INTERNAL ASSESSMENT - 3			
B.E	I	TBA	TBA
B.E	III, V, VII	07-Dec	09-Dec
MCA	III & V	07-Dec	09-Dec
M.Tech	I	TBA	TBA
MCA	I	TBA	TBA

IA — Internal Assessment

IIC — Institution Innovation Council

SEMESTER END EXAMINATIONS

COURSE	START OF EXAM	END OF EXAM
B.E : I - SEM		
B.E : III, V, & VII - SEM	04-01-2021	23-01-2021
M.Tech: I - SEM		
M.Tech: III - SEM	04-01-2021	23-01-2021
MCA: I - SEM		
MCA: III & V - SEM	04-01-2021	23-01-2021

PROFESSIONAL TRAINING/INTERNSHIP VIVA-VOCE

COURSE	START	END	Date
B.E			
M.Tech	III	25-Jan	08-Feb
MCA			
M.Tech	III	22-Feb	

COMMENCEMENT OF EVEN SEMESTER (2020-21)

COURSE	SEM	DATE
B.E	III, V & VII	08-Feb
MCA	III & V	08-Feb
M.Tech	III	22-Feb

ABBREVIATIONS

FIMS — Faculty Information Mgmt. System

FYP — Final Year Project

LIST OF HOLIDAYS

17-Sep	Mahalaya Amavasya
02-Oct	Mahatma Gandhi Jayanthi
26-Oct	Vijayadashami
30-Oct	Eid-Milad
31-Oct	Maharishi Valmiki Jayanti
01-Nov	Kannada Rajyotsava
16-Nov	Balipadyami Deepavali
03-Dec	Kanakadasa Jayanti
25-Dec	Christmas

PARENTS-TEACHERS ASSOCIATION

PTA	DATE
PTA - 1	17-Oct
PTA - 2	TBA

PRACTICAL EXAMINATION

COURSE	SEM	DATES
B.E	III, V, & VII	21-Dec to 31-Dec
MCA	III & V	21-Dec to 31-Dec
M.Tech	III	21-Dec to 31-Dec

PTA — Parents-Teachers-Association

PBL — Projects Based Learning

BMS INSTITUTE OF TECHNOLOGY AND MANAGEMENT

YELAHANKA-BENGALURU-64

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

INDIVIDUAL TIME TABLE FOR THE ACADEMIC YEAR 2020-21 (EVEN SEM)

Name: Dr. Anjan Krishnamurthy	Sub: AC(MT-II), CNSCL (P)	Sem: MTech-II, UG-VI		WEF: 19-04-2021

	I 8.30- 9.30	II 9.30- 10.30	10.30- 10.50	III 10.50- 11.50	IV 11.50.- 12.50	12.50- 1.45	V 1.45-2.40	VI 2.40- 3.35	VII 3.35- 4.30
MONDAY	AC		TEA BREAK	CNSCL		LUNCH BREAK			
TUESDAY	CPL-F2						CNSCL		
WEDNESDAY				AC			CPL-E2		
THURSDAY		CNSCL			AC				
FRIDAY		AC			CNSCL				
SATURDAY				CPL-F1			****		

	Hours	Units
THEORY WORKLOAD	8	16
LABORATORY WORKLOAD	6	6
PG PROJECT WORKLOAD	2	2
UG PROJECT WORKLOAD	4	4
TOTAL WORKLOAD	20	28

BMS INSTITUTE OF TECHNOLOGY AND MANAGEMENT

YELAHANKA, BENGALURU – 64

Department of Computer Science and Engineering

Scroll List of Course Coordinators

Advanced Cryptography (20SCS241)

Sl. No.	Course Coordinator	Course Code	Academic Year	Scheme
1	Dr. Anjan Krishnamurthy	20SCS241	2020-21	2020

VISVESVARAYA TECHNOLOGICAL UNIVERSITY, BELAGAVI
Scheme of Teaching and Examinations – 2020 - 21
M.Tech in Computer Science and Engineering (SCS)
Choice Based Credit System (CBCS) and Outcome Based Education (OBE)

II SEMESTER

SL. No.	Course	Course Code	Course Title	Teaching Hours / Week			Examination				Credits
				Theory	Practical / Seminar	Skill Development Activity	Duration in Hours	CIE Marks	SEE Marks	Total Marks	
1	PCC	20SCS21	Data Science	03	--	02	03	40	60	100	4
2	PCC	20SCS22	Semantic Web and Social Networks	03	--	02	03	40	60	100	4
3	PCC	20SCS23	Blockchain Technology	03	--	02	03	40	60	100	4
4	PEC	20SCS24X	Professional elective 1	04	--	--	03	40	60	100	4
5	PEC	20SCS25X	Professional elective 2	04	--	--	03	40	60	100	4
6	PCC	20SCSL26	Data Science Laboratory	--	04	--	03	40	60	100	2
7	PCC	20SCS27	Technical Seminar	--	02	--	--	100	--	100	2
			TOTAL	**17**	**06**	**06**	**18**	**340**	**360**	**700**	**24**

Note: PCC: Profession Core, PEC: Professional Elective Course

Professional Elective-1		**Professional Elective-2**	
Course Code 20LSCS24X	**Course Title**	**Course Code 20SCS25X**	**Course Title**
20SCS241	Advanced Cryptography	20SCS251	Image Processing and Machine Vision
20SCS242	Natural Language Processing	20SCS252	Object Oriented Design
20SCS243	Cloud Computing	20SCS253	Software Defined Networks
20SCS244	Pattern recognition	20SCS254	Modern Computer Architecture

Note:

1. Technical Seminar: CIE marks shall be awarded by a committee comprising of HoD as Chairman, Guide/co-guide, if any, and a senior faculty of the department. Participation in the seminar by all postgraduate students of the program shall be mandatory.

The CIE marks awarded for Technical Seminar, shall be based on the evaluation of Seminar Report, Presentation skill and performance in Question and Answer session in the ratio 50:25:25.

2. Internship: All the students shall have to undergo mandatory internship of 6 weeks during the vacation of I and II semesters and /or II and III semesters. A University examination shall be conducted during III semester and the prescribed internship credit shall be counted in the same semester. Internship shall be considered as a head of passing and shall be considered for the award of degree. Those, who do not take-up/complete the internship shall be declared as fail in internship course and have to complete the same during the subsequent University examination after satisfying the internship requirements.

Question paper pattern:

The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 60.

- The question paper will have ten full questions carrying equal marks.
- Each full question is for 20 marks.
- There will be two full questions (with a maximum of four sub questions) from each module.
- Each full question will have sub question covering all the topics under a module.
- The students will have to answer five full questions, selecting one full question from each module.
-

Textbook/ Textbooks

1 Mastering Blockchain - Distributed ledgers, decentralization and smart contracts explained, Author- Imran Bashir, Packt Publishing Ltd, Second Edition, ISBN 978-1- 78712-544-5, 2017

Reference Books

1 Bitcoin and Cryptocurrency Technologies, Author- Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder, Princeton University, 2016

2 Blockchain Basics: A Non-Technical Introduction in 25 Steps, Author- Daniel Drescher, Apress, First Edition, 2017

3 Mastering Bitcoin: Unlocking Digital Cryptocurrencies, Andreas M. Antonopoulos, O'Reilly Media, First Edition, 2014

M.TECH IN COMPUTER SCIENCE AND ENGINEERING (SCS) Choice Based Credit System (CBCS) and Outcome Based Education (OBE)			
ADVANCED CRYPTOGRAPHY			
Course Code	**20SCS241**, 20LNI254	CIE Marks	40
Teaching Hours/Week (L:P:S)	4:0:0	SEE Marks	60
Credits	04	Exam Hours	03
Module-1			
Number Theory: Introduction to number theory, Overview of modular arithmetic, discrete logarithms, and primality/factoring, Euclid's algorithm, Finite fields, Prime numbers, Fermat's and Euler's theorem-Testing for primality.			
Module-2			
Symmetric & Asymmetric Cryptography: Classical encryption techniques, Block cipher design principles and modes of operation, Data encryption standard, Evaluation criteria for AES, AES cipher, Principles of public key cryptosystems, The RSA algorithm, Key management – Diffie Hellman Key exchange, Elliptic curve arithmetic-Elliptic curve cryptography.			
Module-3			
Authentication functions:MAC,Hash function, Security of hash function and MAC,MD5,SHA,HMAC, CMAC, Digital signature and authentication protocols, DSS,EI Gamal – Schnorr.			
Module-4			
Authentication applications: Kerberos & X.509 Authentication services Internet Firewalls for Trusted System: Roles of Firewalls , Firewall related terminology-,Types of Firewalls ,Firewall designs, Intrusion detection system , Virus and related threats, Countermeasures , Firewalls design principles ,Trusted systems, Practical implementation of cryptography and security.			
Module-5			
Quantum Cryptography and Quantum Teleportation: Heisenberg uncertainty principle, polarization states of photons, quantum cryptography using polarized photons, local vs. nonlocal interactions,			

BMS INSTITUTE OF TECHNOLOGY AND MANAGEMENT

(Affiliated to the Visvesvaraya Technological University, Belagavi)

Department of Computer Science and Engineering

COURSE DESIGN, DELIVERY AND ASSESMENT

Semester: II

Course Code: 20SCS241

Course Name: Advanced Cryptography

Course Faculty: Dr. Anjan Krishnamurthy

Sl. No.	Section	Course Faculty Name	Signature	Date
1.	2nd Sem M.Tech CSE	Dr. Anjan Krishnamurthy		10/5/2024

Module Coordinator	Signature	Date
Dr. Anjan Krishnamurthy		15/5/2021

Program Coordinator	Signature	Date
Dr. Anjan Krishnamurthy		20/5/2024

Head of Department (Sign & Date)

COUSE DESIGN, DELIVERY AND ASSESSMENT

Course code and title: **Advanced Cryptography**	Course Credits: **(4:0:0) 4**
CIE: **50 Marks**	SEE: **100 Marks**
No. of Theory hours: **50**	Lab support: -
Prepared by: **Dr. Anjan Krishnamurthy**	Date:
Reviewed by:	Date:

Course Preamble:

Prerequisites: Need concepts on basics of number theory and computer networks as the prerequisites for this course.

Course Objectives:

1. To explain standard algorithms used to provide confidentiality, integrity and authenticity.
2. To distinguish key distribution and management schemes.
3. To deploy encryption techniques to secure data in transit across data networks
4. To implement security applications in the field of Information technology

Syllabus/Course contents:

MODULE I

Number Theory: Introduction to number theory, Overview of modular arithmetic, discrete logarithms, and primality/factoring, Euclid's algorithm, Finite fields, Prime numbers, Fermat's and Euler's theorem- Testing for primality.

MODULE II

Symmetric & Asymmetric Cryptography: Classical encryption techniques, Block cipher design principles and modes of operation, Data encryption standard, Evaluation criteria for AES, AES cipher, Principles of public key cryptosystems, The RSA algorithm, Key management — Diffie Hellman Key exchange, Elliptic curve arithmetic-Elliptic curve cryptography.

MODULE III

Authentication functions: MAC, Hash function, Security of hash function and MAC,MD5,SHA,HMAC, CMAC, Digital signature and authentication protocols, DSS,EI Gamal — Schnorr

MODULE IV

Authentication applications: Kerberos & X.509 Authentication services Internet Firewalls for Trusted System: Roles of Firewalls, Firewall related terminology-,Types of Firewalls ,Firewall

designs, Intrusion detection system , Virus and related threats, Countermeasures , Firewalls design principles ,Trusted systems, Practical implementation of cryptography and security.

MODULE V

Quantum Cryptography and Quantum Teleportation: Heisenberg uncertainty principle, polarization states of photons, quantum cryptography using polarized photons, local vs. Nonlocal interactions, entanglements, EPR paradox, Bell's theorem, Bell basis, teleportation of a single qubit theory and experiments.

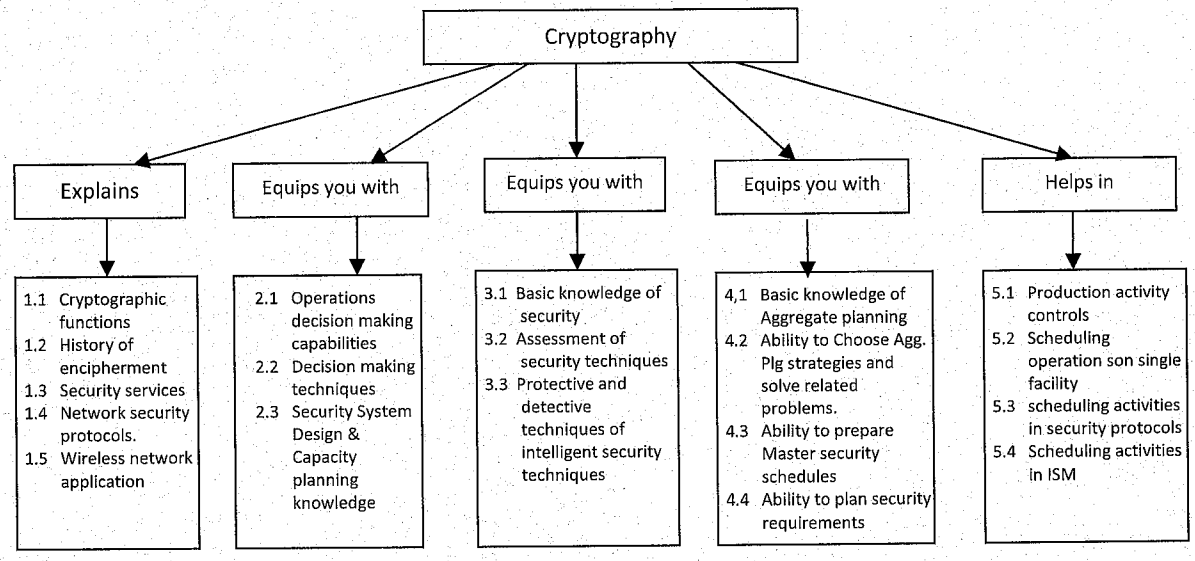
Textbooks:

1. Cryptography and Network Security Principles And Practice William Stallings Pearson Education Fourth Edition
2. A Course in Number Theory and Cryptology, Neal Koblitz, Springer, 1987

Reference Books:

1. QuantumComputation and Quantum Information, Michael A. Nielsen and Issac L Chuang, Cambridge University Press 10th Anniversary Edition Hardcover, Illustrated 2010.

Concept Map



M.Tech Program Educational Objectives (PEOs)

PEO1 Apply analytical thinking to solve problems through research in the areas of Computer Science and Engineering.

PEO2 Adapt to changing technological trends through life-long learning by exhibiting professional ethics, integrity and career growth.

PEO3 Develop skills to facilitate in providing sustainable solutions by addressing the ever-growing challenges of the society.

M.Tech Program Outcomes (POs)

The graduates of M. Tech. in Computer Science and Engineering (CSE) Program will be able to:

PO1 Independently carry out research and development work to solve practical problems related to Computer Science and Engineering domain.

PO2 Write and present a substantial technical report/document.

PO3 Demonstrate a degree of mastery over the area as per the specialization of the program. The mastery should be at a level higher than the requirements in the appropriate bachelor program.

PO4 Analyze the acquired domain knowledge for providing feasible solution(s).

PO5 Relate the learning outcomes to build requisite competency in professional environment.

PO6 Appraise the need for engaging in lifelong learning.

Course Contents and Lecture Schedule:

Lesson/ Session No.	Topics	No. of Hours
1.	**Introduction to number theory**	1
2.	Overview of modular arithmetic,	1
3.	Overview of modular arithmetic,	1
4.	Euclid's algorithm,	1
5.	Euclid's algorithm,	1
6.	discrete logarithms, and primality/factoring,	1
7.	Finite fields, Prime numbers,	1
8.	Finite fields, Prime numbers,	1
9.	Fermat's and Euler's theorem-.	1
10.	Testing for primality	1
11.	**Introduction to Classical encryption techniques,**	1
12.	Classical encryption techniques,	1
13.	Classical encryption techniques,	1
14.	Block cipher design principles and modes of operation, Data encryption standard,	1
15.	Block cipher design principles and modes of operation, Data encryption standard,	1
16.	Evaluation criteria for AES, AES cipher,	1
17.	Principles of public key cryptosystems, The RSA algorithm,	1
18.	Principles of public key cryptosystems, The RSA algorithm,	1
19.	Key management — Diffie Hellman Key exchange,	1
20.	Elliptic curve arithmetic-Elliptic curve cryptography.	1
21.	**Authentication functions Introduction**	1
22.	MAC,	1
23.	Hash function, Security of hash function	1
24.	Hash function, Security of hash function	1
25.	MAC,MD5,	1
26.	MAC,MD5,	1
27.	SHA,HMAC, CMAC,	1
28.	SHA,HMAC, CMAC,	1
29.	Digital signature and authentication protocols,	1
30.	DSS,El Gamal — Schnorr	1
31.	**Authentication applications:**	1
32.	Kerberos	1
33.	X.509 Authentication services	1
34.	Internet Firewalls for Trusted System: Roles of Firewalls,	1
35.	Firewall related terminology-,Types of Firewalls ,	1
36.	Firewall designs, Intrusion detection system ,	1

37.	Virus and related threats,	1
38.	Countermeasures , Firewalls design principles ,	1
39.	Trusted systems,	1
40.	Practical implementation of cryptography and security.	1
41.	**Quantum Cryptography and Quantum Teleportation: Introduction**	1
42.	Heisenberg uncertainty principle,	1
43.	polarization states of photons,	1
44.	quantum cryptography using polarized photons	1
45.	Local vs. Nonlocal interactions, entanglements,	1
46.	Local vs. Nonlocal interactions, entanglements,	1
47.	EPR paradox,	1
48.	Bell's theorem, Bell basis,	1
49.	Bell's theorem, Bell basis	1
50.	Teleportation of a single qubit theory and experiments.	1
	Total No. of Lecture Hours	**50**

Course Delivery Plan

Week	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
	I II	I II	I II	I II	I II	I II	I II	I II	I II	I II	I II	I II	I II	I II	I II	I II
Units		1			2			3			4				5	

Course Delivery:

Chalk & Black board, Interactions, Simulation in Lab and Case analysis.

Course Outcomes:

CO No.	Course Outcome	BT Levels
MCSE.1241.1	Apply the basic modular arithmetic concepts and set theory properties in cryptographic algorithms for encryption and decryption, hash functions, PRNGS.	K3
MCSE.1241.2	Identify suitable firewall and authentication mechanism for real time protection against any attacks.	K4
MCSE.1241.3	Evaluate the strength of cryptographic algorithms based on attack modeling and publish results.	K5
MCSE.1241.4	Develop exploratory study in analyzing the potential impact on futuristic development of cryptographic system in the areas of quantum cryptography, DNA cryptography.	K6

Mapping Course Outcomes with Program Outcomes:

CO No.	Course Outcome	PO1	PO2	PO3	PO4	PO5	PO6
MCSE.1241.1	Apply the basic modular arithmetic concepts and set theory properties in cryptographic algorithms for encryption and decryption, hash functions, PRNGS.			3			
MCSE.1241.2	Identify suitable firewall and authentication mechanism for real time protection against any attacks.				3		
MCSE.1241.3	Evaluate the strength of cryptographic algorithms based on attack modeling and publish results.	2	2			3	
MCSE.1241.4	Develop exploratory study in analyzing the potential impact on futuristic development of cryptographic system in the areas of quantum cryptography, DNA cryptography.						2

Assessment of Course Outcomes:

		What	Frequency	Max Marks	Evidence collected	Course Outcomes
Direct Assessment Methods	CIE	Internal assessment tests	Thrice (Average of all the three tests will be considered)	20	Blue books	1,2,4
		Class-room open book assignment	Once	20	Assignment reports	3
	SEE	Standard examination covering full syllabus	Once at the End of course	100	Answer scripts	1, 2 and 4
Indirect Assessment Methods		Students feedback about the Delivery of the course	Twice during the course	-	Feedback forms	All COs
		End of course survey (On Course contents, Quality of Delivery and Assessment methods)	Once at the End of course	-	Response through Questionnaire	All COs

Course Evaluation:

Questions for CIE and SEE will be designed to evaluate cognitive skills the various educational levels (Bloom's taxonomy) such as:

Sl. No.	Bloom's category	Test 1	Test 2	Test 3	SEE
1.	Remember	--	--	--	20
2.	Understand	15	15	15	20
3.	Apply	15	15	10	20
4.	Analyze	10	10	10	20
5.	Evaluate	10	10	10	15
6.	Create	0	0	5	5

Course Unitization for Internals and Semester End Examination

Part	Modules		Teaching Hours	No. of Questions in		
				Internals I	Internals II	Internals III
Unit 1	1	Number Theory	10	4+1*		
Unit 2	2	Symmetric & Asymmetric Cryptography	10	2+1*	1	
Unit 3	3	Authentication functions	10		3+1*	
Unit 4	4	Authentication applications	10		2+1*	2+1*
Unit 5	5	Quantum Cryptography and Quantum Teleportation	10			4+1*

*Represents Innovative and Case Study questions from the units

IA Scheme

Assessment	Weightage in Marks
3 IA test	50
IA average	50 (20)
Assignment	20
Total	**40**

Sample Question Paper for IA Test 1

BMS INSTITUTE OF TECHNOLOGY AND MANAGEMENT

Avalahalli, Doddaballapur Main Road, Bengaluru - 560064

FIRST INTERNAL ASSESSMENT TEST, JUN 2020 - 21

Name of the Course	Advanced Cryptography	Course Code	20SCS241
Branch & Semester	2nd Sem M.Tech CSE	Date	29-06-2021 (2:00PM-3:30PM)
Name of the Course Coordinator	Dr. Anjan Krishnamurthy	Max. Marks	50

Portions for the IA/Test:

MODULE I

Number Theory: Introduction to number theory, Overview of modular arithmetic, discrete logarithms, and primality/factoring, Euclid's algorithm, Finite fields, Prime numbers, Fermat's and Euler's theorem- Testing for primality.

MODULE II

Symmetric & Asymmetric Cryptography: Classical encryption techniques, Block cipher design principles and modes of operation, Data encryption standard, Evaluation criteria for AES, AES cipher, Principles of public key cryptosystems, The RSA algorithm, Key management — Diffie Hellman Key exchange, Elliptic curve arithmetic-Elliptic curve cryptography.

Course Outcomes to be assessed in this Internal Assessment:

CO1: Apply the basic modular arithmetic concepts and set theory properties in cryptographic algorithms for encryption and decryption, hash functions, PRNGS. (K3)

CO2: Identify suitable firewall and authentication mechanism for real time protection against any attacks. (K4)

CO3: Evaluate the strength of cryptographic algorithms based on attack modeling and publish results.(K5)

CO4: Develop exploratory study in analyzing the potential impact on futuristic development of cryptographic system in the areas of quantum cryptography, DNA cryptography. (K6)

Instructions to Candidates: Answer all the questions

Qn. No.		CO
1.	Compute the ***Modulo*** – *7* table for additive and multiplicative operations and identify which of the tables conforms to basic set properties.	**CO1, K3**
2.	Apply the extended Euclidean algorithm for determining the inverse of **550** using **GF(1759).** Trace the algorithm at every step for the variables Q, A_1, A_2, A_3, B_1, B_2, B_3.	**CO1, K3**
3.	Illustrate the use of polynomial arithmetic to compute **GF(2^3)** by provide the addition modulo and multiplicative module tables. Highlight on the computational considerations made for this calculation.	**CO1,K3**
4.	Apply the Diffie Hellman key exchange algorithms for the values given below i. **q=287, α = 7, X_a= 91, X_b= 257** ii. **q= 353, α = 3, X_a= 97, X_b= 233**	**CO1, K3**
5.	Identify various attacks feasible on RSA algorithm provided the chosen primes are of the size 50 digits / 256bits.	**CO3, K4**
6.	Apply the One-time pad encryption for the plain text and key given below – **Plain Text: Information Science and Engineering** **Key - HL MS EZ RB HP SJ OT DW**	**CO1, K3**
7.	Prove that if n>2 and p_I=y_{mI} then m_I=0 where p is prime number and m_I and y_m are the intervals ranging from 0 to n.	**CO3, K5**
8.	Construct the Sieve of Eratosthenes for numbers up to 50. Show stepwise elimination of non-prime numbers. How can this method be used for RSA prime factorization?	**CO3, K5**

Internal Assessment- I: Scheme and Solution (Must be provided)

Qn. No.	PART A	Marks
1.	Modulo – 7 Table for addition and multiplication group (6)	10 M

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

*	0	1	2	3	4	5	6

	0 0 0 0 0 0 0 0 **1** 0 1 2 3 4 5 6 **2** 0 2 4 6 1 3 5 **3** 0 3 6 2 5 1 4 **4** 0 4 1 5 2 6 3 **5** 0 5 3 1 6 4 2 **6** 0 6 5 4 3 2 1 Set properties (4)	
	OR	
2.	Extended Euclidean Algorithm (6) Table (4) **Q A1 A2 A3 B1 B2 B3** — 1 0 1759 0 1 550 3 0 1 550 1 –3 109 5 1 –3 109 –5 16 5 21 –5 16 5 106 –339 4 1 106 –339 4 –111 355 1	10 M
3.	Polynomial Arithmetic (7) Computation consideration (3)	10 M
	OR	
4.	**1. Ya= 63** **Yb= 112** **Kab = 147** **2. Ya= 40** **Yb= 248** **Kab = 160** **5x2=10**	10 M
5.	Attacks on RSA Algorithm (6) Chosen Prime explanation (4)	10 M
	OR	
6.	One time Pad Key - HL MS EZ RB HP SJ OT DW 0812 1319 0526 1802 0816 1910 1520 0423 A B C D E F G H I J K L M N O P Q R S 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 T U V W X Y Z 20 21 22 23 24 25 26	10 M

	Plain Text: Information Science and Engineering (3) 09 14 0615 18 13 01 20 09 15 141903 0905 1403 0501 1404 0514 0709 1405 0518 0914 0724 one time pad cipher text: (7) 0127 2625 2646 1310 1719 1815 2923 0924 1216 1823 0225 2207 0324 1824 1344 0812 1319 0526 1802 0816 1910 1520 0423 0812 1319 0526 1802 0816 1910 1520 0315 1316 2120 0518 1903 0905 1403 0501 1404 0514 0709 1405 0518 0914 0724	
	PART B	
7.	Proof (6) Prime number theory (4)	10 M
8.	Sieve of Eratosthenes Table (4) Stepwise elimination (3) RSA Primes (3)	10 M

Details of the Innovative teaching methods:

Topic	Unit	Book	ITM
Cyberstalking, Cybercafe and Cybercrimes, Botnets: The Fuel for Cybercrime, Attack Vector, Cloud Computing https://www.youtube.com/watch?v=aKaFqS2Q39E	1	R1	Flipped Mode
Credit Card Frauds in Mobile and Wireless Computing Era https://www.youtube.com/watch?v=MdAZPTiy6fQ	2	R1	Flipped Mode
Virus and Worms, Trojan Horses https://www.youtube.com/watch?v=y8a3QoTg4VQ	3	R1	Flipped Mode
Need for An Information Security Policy https://www.youtube.com/watch?v=_5AFRQo4JwU	4	R1	Flipped Mode
Social Networking Sites: The Security/Privacy Threats https://www.youtube.com/watch?v=SKBR1CaP80U	5	R1	Flipped Mode

Assignment Rubrics

Dimension	Maximum Marks	High	Medium	Low
Introduction		Position and exceptions, if any, are clearly stated. Organization of the argument is completely and clearly outlined and implemented.	Position is clearly stated. Organization of argument is clear in parts or only partially described and mostly	Position is vague. Organization of argument is missing, vague, or not consistently maintained.

			implemented.	
	5	**4-5 pts**	**2-3 pts**	**0-1 pts**
Research		Research selected is highly relevant to the argument, is presented accurately and completely – the method, results, and implications are all presented accurately; Theory is relevant, accurately described and all relevant components are included; relationship between research and theory is clearly articulated and accurate.	Research is relevant to the argument and is mostly accurate and complete – there are some unclear components or some minor errors in the method, results or implications. Theory is relevant and accurately described, some components may not be present or are unclear. Connection to theory is mostly clear and complete, or has some minor errors.	Research selected is not relevant to the argument or is vague and incomplete – components are missing or inaccurate or unclear. Theory is not relevant or only relevant for some aspects; theory is not clearly articulated and/or has incorrect or incomplete components. Relationship between theory and research is unclear or inaccurate, major errors in the logic are present.
	5	**4-5 pts**	**2-3 pts**	**0-1 pts**
Conclusions		Conclusion is clearly stated and connections to the research and position are clear and relevant. The underlying logic is explicit. 4-5 pts	Conclusion is clearly stated and connections to research and position are mostly clear,	Conclusion may not be clear and the connections to the research are incorrect or unclear or just a repetition of the findings

			some aspects may not be connected or minor errors in logic are present.	without explanation. Underlying logic has major flaws; connection to position is not clear.
	5	**4-5 pts**	**2-3 pts**	**0-1**
Writing		Paper is coherently organized and the logic is easy to follow. There are no spelling or grammatical errors and terminology is clearly defined. Writing is clear and concise and persuasive.	Paper is generally well organized and most of the argument is easy to follow. There are only a few minor spelling or grammatical errors, or terms are not clearly defined. Writing is mostly clear but may lack conciseness.	Paper is poorly organized and difficult to read – does not flow logically from one part to another. There are several spelling and/or grammatical errors; technical terms may not be defined or are poorly defined. Writing lacks clarity and conciseness.
	5	**4-5 pts**	**2-3 pts**	**0-1**

Model Questions

1 What is cryptanalysis? Explain different types of cryptanalysis attack.

2 Using the keyword "SUMMER" , construct an playfair matrix and encrypt the message "LOCKER ROOM"

3 Encrypt the message "SPRING" using the below 3x3 key matrix –

17	**17**	**5**
21	**18**	**21**
2	**2**	**19**

4 Given 10-bit key is **1010111101**. The permutation

P10 = (3 5 2 7 4 10 1 9 8 6) and P8 = (6 3 7 4 8 5 10 9).

Generate subkeys K_1 and K_2 using Simplified DES and encrypt the 8-bit plain text 10111100 using the generated keys. Draw a block diagram depicting the SDES process.

5 Write RSA algorithm in steps. Discuss about various security issues of the algorithm. Also perform encryption and decryption for

(i) p=7,q=11,e=17,M=8.

(ii) p=17,q=31,e=7,M=2

6 Apply Mono-alphabetic cipher to decrypt the message given below –

```
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
```

The relative frequency of all the letters in English is given the table below –

A	8.16	**B**	1.49	**C**	2.73	**D**	4.25	**E**	12.73	**F**	2.22	**G**	2.01	**H**	6.09
I	6.99	**J**	0.15	**K**	0.77	**L**	4.02	**M**	2.4	**N**	6.74	**O**	7.5	**P**	1.92
Q	0.09	**R**	5.98	**S**	6.32	**T**	9.05	**U**	2.75	**V**	0.97	**W**	2.36	**X**	0.15
Y	1.97	**Z**	0.07												

7 With the help of neat block diagram, describe the characteristics and principles of feistel cipher structure.

8 Explain the principles of the Block Cipher algorithms.

9 In a public-key system using RSA, you intercept the ciphertext C = 10 sent to a user whose public key is e = 5, n = 35.What is the plaintext M?

10 **Write a note on:** (use appropriate examples wherever applicable)

i. One time pad

ii. Confusion and Diffusion

iii. Avalanche effect in DES algorithm

11 Give the format of SSL Record protocol and mention the SSL architectural characteristics of SSL.

12 List the permitted cipher algorithms in SSL.

13 With neat diagram, Discuss the handshaking process in SSL.

14 What is RSN service? List the RSN services and protocol supported in RSN.

15 With Neat flow diagram, describe the working of PGP message generation and extraction at the receiver's end.

16 With neat diagram, describe the ESP mode of IPSec and also mention the working of IPsec in tunnel and transport modes (ESP format).

17 List the different stages and of IPSec Key management and describe the IKE key determination protocol.

18 Give different scenarios of combining security associations in IP Sec.

19 What is Security Parameter Index (SPI) in IPSec?

20 Elaborate on key management phase in 802.11i and also list the various protocols supported in this phase.

21 With a neat diagram, give the working of PRNG function in 802.11i

22 Describe different phases of operation in 802.11i. Use appropriate diagram wherever required.

23 With a suitable example, explain the working of Diffie-Hellman key exchange protocol.

24 Consider an ElGamal scheme with a common prime q= 71 and a primitive root with $\alpha = 7$.

i. If B has public key Y_B=3and A chose the random integer k=2 and M =30, Calculate the cipher text?

ii. If A chooses a different value k and M=30 then C=(59,C_2), what is the integer C_2?

25 Give the PRNG generation method. Describe at-least one algorithm to generate the PRNG.

26 What is realm? Explain Kerberos V4 realm authentication mechanism. Differentiate Kerberos V5 over Kerberos V4.

27 Prove that Z_8 is not Finite Field under (*,+).

28 Prove the point E(1,1) with x=9 and y=7 is point on the curve $y^2 = x^3 + x + 1$. For the point P (3,1) and Q (4,6), give P+Q and 2P.

29 Illustrate with examples the different types of Hybrid scheme of key distribution.

30 What is Security Parameter Index (SPI) in IPSec? Give different scenarios of combining security associations in IP Sec.

Course End Survey questions

Advanced Cryptography (20SCS241)

SNo	Questions	PO
1.	Did the course allow you to independently think to solve problems related to advanced cryptographic algorithms leading to research work? (Yes/No)	1
2.	Did the course enable you to articulate, present, write reports or documents?	2
3.	Rate the level of your mastery over the course before taking it. (1-Low, 2- Medium, 3 -High)	3
4.	Rate the level of your mastery over the course after taking it. (1-Low, 2- Medium, 3 -High)	3
5.	Are the topics in this course appropriately assisted you in identifying solution?	4
6.	Were you able to do research work in the field of computer science aligned with your course where the work showcases your leadership, integrity and professional ethics?	5
7.	Did make use of the any research tools for security?	5
8.	To what extent you grade the quality of contents in this subject?	6
9.	Do you feel topics included in this course will give good background for higher education?	6
10.	Rate the level of the knowledge improvement after the successful completion of this course. (1-Low, 2- Medium, 3 -High)	6

BMS INSTITUTE OF TECHNOLOGY AND MANAGEMENT
YELAHANKA – BANGALORE - 64
DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

Minutes of Meeting with PAC –Batch 2020-22

Date	20 -05-2021	Location	Online
Time	10:30am	Module Coordinator	Dr. Anjan Krishnamurthy
Course Name	Current Course Coordinator	Previous Course Coordinator	
Advanced Cryptography 20SCS241	Dr. Anjan Krishnamurthy	--	

Sl. No	Discussion	Action By/ Responsible	Action Taken
1	**Agenda:** Course Outcomes, CO – PO Mapping, Gap Identification for Advanced Cryptography (20SCS241)		

The **Course Outcomes (COs)** for **Advanced Cryptography** given in university curriculum are as follows:

Course Coordinator

CO No.	Course Outcome	BT Level
MCSE.1241.1	Understand OSI security architecture and classical encryption techniques	K1
MCSE.1241.2	Acquire fundamental knowledge on the concepts of finite fields and number theory	K2
MCSE.1241.3	Understand various block cipher and stream cipher models	K1
MCSE.1241.4	Describe the principles of public key cryptosystems, hash functions and digital signature	K1
MCSE.1241.5	Compare various Cryptographic Techniques	K4
MCSE.1241.6	Design Secure applications	K6
MCSE.1241.7	Inject secure coding in the developed applications	K6

Existing University CO's Mapping with POs

CO No.	Course Outcome	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6
MCSE.1241.1	Understand OSI security architecture and classical encryption techniques						
MCSE.1241.2	Acquire fundamental knowledge on the concepts of finite fields and number theory						
MCSE.1241.3	Understand various block cipher and stream cipher models						
MCSE.1241.4	Describe the principles of public key cryptosystems, hash functions and digital signature						
MCSE.1241.5	Compare various Cryptographic Techniques				1		
MCSE.1241.6	Design Secure applications					1	
MCSE.1241.7	Inject secure coding in the developed applications						1

The Observations of the committee are as follows:

1. The first four **MCSE.1241.1 to MCSE.1241.4** COs drafted by the university do not map to any POs set by NBA and Dept. and therefore there is not learning contribution to the attainment of the POs.
2. The COs drafted are observed to be variably to different revised Blooms's taxonomy level and are not in ordered sequence like CO1- K2, CO2-K3 and so on.
3. The last three COs do not map at the required level to the POs.
4. The COs do not have skill words for better mapping with POs.
5. No COs to highlight the research skills which is major component in PO1.
6. No COs to map to advanced level topics of cryptography.

Gap identified:

Gaps are identified for all POs and some POs have low mapping.

Redefined COs-

CO No.	Course Outcome	BT Levels
MCSE.1241.1	Apply the basic modular arithmetic concepts and set theory properties in cryptographic algorithms for encryption and decryption, hash functions, PRNGS.	K3
MCSE.1241.2	Identify suitable firewall and authentication mechanism for real time protection against any attacks.	K4
MCSE.1241.3	Evaluate the strength of cryptographic algorithms based on attack modeling and publish results.	K5
MCSE.1241.4	Develop exploratory study in analyzing the potential impact on futuristic development of cryptographic system in the areas of quantum cryptography, DNA cryptography.	K6

CO-PO Mapping

CO No.	Course Outcome	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6
MCSE.1241.1	Apply the basic modular arithmetic concepts and set theory properties in cryptographic algorithms for encryption and decryption, hash functions, PRNGS.			3			
MCSE.1241.2	Identify suitable firewall and authentication mechanism for real time protection against any attacks.				3		
MCSE.1241.3	Evaluate the strength of cryptographic algorithms based on attack modeling and publish results.	2	2			3	
MCSE.1241.4	Develop exploratory study in analyzing the potential impact on futuristic development of cryptographic system in the areas of quantum cryptography, DNA						2

		cryptography.								

Articulation:

- CO1 maps to PO3 medium as it application of mathematical modelling to cryptographic application.
- CO2 maps to PO4 medium as it deals with professional competency in using firewalls and authentication systems for security applications.
- CO3 maps to PO1, PO2 and PO5 as it deals with cryptanalysis and cryptographic study of an algorithm under development or research. This can be based on rigorous testing on various attack environment that to bleak the CIA pillar of security.
- CO4 maps to PO5 and PO6 medium as this shall be advancement beyond the traditional white box cryptographic system that is merely based on digital computing and could have lifelong engagement of research in the field of Quantum and DNA computing applications.

3	**Action planned to bridge the gap** • To deepen the knowledge in the domain a workshop/ MOOC shall be conducted for improved mapping with POs (1,2,3) • Cooperative learning with incidental approach shall be incorporated in the teaching learning process to enhance the PO mapping to better level.		Research topics in new age cryptographic algorithm

Final CO-PO Mapping

CO No.	Course Outcome	PO1	PO2	PO3	PO4	PO5	PO6
MCSE.1241.1	Apply the basic modular arithmetic concepts and set theory properties in cryptographic algorithms for encryption and decryption, hash functions, PRNGS.			3			
MCSE.1241.2	Identify suitable firewall and authentication mechanism for real time protection against any attacks.				2		
MCSE.1241.3	Evaluate the strength of cryptographic algorithms based on attack modeling and publish results	2	2			3	
MCSE.1241.4	Develop exploratory study in analyzing the potential impact on futuristic development of cryptographic system in the areas of quantum cryptography, DNA cryptography.						2

10/5/2021 20/5/2021

Course Coordinator **Program Coordinator** **HoD-CSE**

Dr. Anjan Krishnamurthy
Associate Professor
Dept. of CSE,
BMS Institute Of Technology & Management
Avalahalli Yelahanka, Bengaluru-560

BMS INSTITUTE OF TECHNOLOGY, YELAHANKA, BANGALORE-64

PROVISIONAL SECTION LIST

PG COURSE : COMPUTER SCIENCE AND ENGINEERING

SL. NO	USN	NAME OF THE CANDIDATE
1.	1BY20SCS01	ADITHYA SHARMA B S
2.	1BY20SCS02	ARUNKUMAR K BHAVIKATTI
3.	1BY20SCS03	BHAVANA G V
4.	1BY20SCS04	CHERUKU YASASWINI
5.	1BY20SCS05	PRAGNA M V
6.	1BY20SCS06	PRIYANKA
7.	1BY20SCS08	SRIDHAR H S
8.	1BY20SCS09	TEJASWINI HALAKATE
9.	1BY20SCS10	UMME AYMUN

PRINCIPAL
BMS Inst.of Tech.& Mgmt.
Doddaballapur Main Road
Avalahalli,Yelahanka, B'lore-64

BMS INSTITUTE OF TECHNOLOGY AND MANAGEMENT

Avalahalli, Doddaballapur Main Road, Bengaluru - 560064

FIRST INTERNAL ASSESSMENT TEST, JUN 2020 - 21

Name of the Course	Advanced Cryptography	Course Code	20SCS241
Branch & Semester	2nd Sem M.Tech CSE	Date	29-06-2021 (2:00PM-3:30PM)
Name of the Course Coordinator	Dr. Anjan Krishnamurthy	Max. Marks	50

Note: *Answer* ***THREE*** *full questions from* ***Part A*** *and* ***Part B*** *questions are compulsory.*

Qn. No.	PART A	Marks	CO
1.	Compute the ***Modulo – 7*** table for additive and multiplicative operations and identify which of the tables conforms to basic set properties.	10 M	CO1, K3
	OR		
2.	Apply the extended Euclidean algorithm for determining the inverse of **550** using **GF(1759)**. Trace the algorithm at every step for the variables Q, A_1, A_2, A_3, B_1, B_2, B_3.	10 M	CO1, K3
3.	Illustrate the use of polynomial arithmetic to compute **GF(2^3)** by provide the addition modulo and multiplicative module tables. Highlight on the computational considerations made for this calculation.	10 M	CO1,K3
	OR		
4.	Apply the Diffie Hellman key exchange algorithms for the values given below i. **q=287, α = 7, X_a= 91, X_b= 257** ii. **q= 353, α = 3, X_a= 97, X_b= 233**	10 M	CO1, K3
5.	Identify various attacks feasible on RSA algorithm provided the chosen primes are of the size 50 digits / 256bits.	10 M	CO3, K4
	OR		
6.	Apply the One-time pad encryption for the plain text and key given below – **Plain Text: Information Science and Engineering** **Key - HL MS EZ RB HP SJ OT DW**	10 M	CO1, K3
	PART B		
7.	**Innovative question** Prove that if n>2 and $p_1=y_{m1}$ then $m_1=0$ where p is prime number and m_1 and y_m are the intervals ranging from 0 to n.	10 M	CO3, K5
8.	**Case Study Question** Construct the Sieve of Eratosthenes for numbers up to 50. Show stepwise elimination of non-prime numbers. How can this method be used for RSA prime factorization?	10 M	CO3, K5

Course Outcomes (COs)

CO1:	Apply the basic modular arithmetic concepts and set theory properties in cryptographic algorithms for encryption and decryption, hash functions, PRNGS. (K3)
CO2:	Identify suitable firewall and authentication mechanism for real time protection against any attacks. (K4)
CO3:	Evaluate the strength of cryptographic algorithms based on attack modeling and publish results.(K5)
CO4:	Develop exploratory study in analyzing the potential impact on futuristic development of cryptographic system in the areas of quantum cryptography, DNA cryptography. (K6)

Revised Bloom's Category

Remembering (K1)	Understanding (K2)	Applying (K3)	Analyzing (K4)	Evaluating (K5)	Creating (K6)

Signatures of the Question Paper Scrutiny Committee

Course Coordinator(s)	Module Coordinator(s)	Program Coordinator	Head of the Department
28/6/2021	28/6/2021	28/6/2021	

BMS INSTITUTE OF TECHNOLOGY AND MANAGEMENT

Avalahalli, Yelahanka, Doddaballapura Main Road, Bengaluru - 560064

FIRST ASSESSMENT TEST, Jun2020 - 21

Name of the Course	Advanced Cryptography	Course Code	20SCS241
Branch & Semester	2nd Sem M.Tech CSE	Date	29-06-2021 (2:00PM-3:30PM)
Name of the Course Coordinator	Dr. Anjan Krishnamurthy	Max. Marks	50

Scheme and Solution

Qn. No.	PART A	Marks
1.	Modulo – 7 Table for addition and multiplication group (6)	10 M

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

*	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Set properties (4)

OR

2.	Extended Euclidean Algorithm (6) Table (4)	10 M

Q	A1	A2	A3	B1	B2	B3
—	1	0	1759	0	1	550
3	0	1	550	1	–3	109
5	1	–3	109	–5	16	5
21	–5	16	5	106	–339	4
1	106	–339	4	–111	355	1

3.	Polynomial Arithmetic (7) Computation consideration (3)	10 M

OR

4.	**1. Ya= 63** **Yb= 112** **Kab = 147** **2. Ya= 40** **Yb= 248** **Kab = 160**	10 M

	5x2=10	
5.	Attacks on RSA Algorithm (6) Chosen Prime explanation (4)	10 M
	OR	
6.	One time Pad Key - HL MS EZ RB HP SJ OT DW 0812 1319 0526 1802 0816 1910 1520 0423 A B C D E F G H I J K L M N O P Q R S 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 T U V W X Y Z 20 21 22 23 24 25 26 Plain Text: Information Science and Engineering (3) 09 14 0615 18 13 01 20 09 15 141903 0905 1403 0501 1404 0514 0709 1405 0518 0914 0724 one time pad cipher text: (7) 0127 2625 2646 1310 1719 1815 2923 0924 1216 1823 0225 2207 0324 1824 1344 0812 1319 0526 1802 0816 1910 1520 0423 0812 1319 0526 1802 0816 1910 1520 0315 1316 2120 0518 1903 0905 1403 0501 1404 0514 0709 1405 0518 0914 0724	10 M
	PART B	
7.	Proof (6) Prime number theory (4)	10 M
8.	Sieve of Eratosthenes Table (4) Stepwise elimination (3) RSA Primes (3)	10 M

BMS INSTITUTE OF TECHNOLOGY AND MANAGEMENT

Avalahalli, Doddaballapur Main Road, Bengaluru - 560064

SECOND INTERNAL ASSESSMENT TEST, AUG 2020 - 21

Name of the Course	Advanced Cryptography	Course Code	20SCS241
Branch & Semester	2nd Sem M.Tech CSE	Date	27-08-2021 (2:00PM-3:30PM)
Name of the Course Coordinator	Dr. Anjan Krishnamurthy	Max. Marks	50

Note: *Answer* ***THREE*** *full questions from* ***Part A*** *and* ***Part B*** *questions are compulsory.*

Qn. No.	PART A	Marks	CO
1.	Prove the point E(1,1) with x=9 and y=7 is point on the curve $y^2 = x^3 + x + 1$. For the point P (3,1) and Q (4,6), give P+Q and 2P	10 M	CO3, K5
	OR		
2.	Summarize the properties of the cryptographic hash function.	10 M	CO1, K2
3.	With value of q=19 and a = 10, construct an ElGamal Signature scheme using GF(19). Choose random key as K=5, X_A=16.	10 M	CO3,K4
	OR		
4.	Illustrate the working of HMAC with examples.	10 M	CO3, K3
5.	Differentiate Kerberos V5 over Kerberos V4. Explain the Kerberos V4 realm authentication mechanism.	10 M	CO2, K4
	OR		
6.	Illustrate the working of El Gamal – Schrorr scheme with examples.	10 M	CO3, K3
	PART B		
7.	**Innovative question** UAE Smart ID card uses the PKI mechanism for the authentication and encryption. Design the public key certificate for smart ID card using X.509. Illustrate the security services that shall be provided by the smart card.	10 M	CO4, K5
8.	**Case Study Question** Relate the correlation of the intrusion detection systems with that cryptographic hash. Highlight the various stages of intrusion detection systems where hash values are processed.	10 M	CO3, K5

Course Outcomes (COs)

CO1:	Apply the basic modular arithmetic concepts and set theory properties in cryptographic algorithms for encryption and decryption, hash functions, PRNGS. (K3)
CO2:	Identify suitable firewall and authentication mechanism for real time protection against any attacks. (K4)
CO3:	Evaluate the strength of cryptographic algorithms based on attack modeling and publish results.(K5)
CO4:	Develop exploratory study in analyzing the potential impact on futuristic development of cryptographic system in the areas of quantum cryptography, DNA cryptography. (K6)

Revised Bloom's Category

Remembering (K1)	Understanding (K2)	Applying (K3)	Analyzing (K4)	Evaluating (K5)	Creating (K6)

Signatures of the Question Paper Scrutiny Committee

Course Coordinator(s)	Module Coordinator(s)	Program Coordinator	Head of the Department

BMS INSTITUTE OF TECHNOLOGY AND MANAGEMENT

Avalahalli, Yelahanka, Doddaballapura Main Road, Bengaluru - 560064

SECOND ASSESSMENT TEST, Aug 2020 - 21

Name of the Course	Advanced Cryptography	Course Code	20SCS241
Branch & Semester	2nd Sem M.Tech CSE	Date	27-08-2021 (2:00PM-3:30PM)
Name of the Course Coordinator	Dr. Anjan Krishnamurthy	Max. Marks	50

Scheme and Solution

Qn. No.	PART A	Marks
1.	Solve the point using the given equation (4) $y^2 \equiv x^3 + x + 6 \pmod{11}$ lies the point $P = (2, 7) = (x1, y1)$ Indeed, $49 \equiv 16 \bmod 11$. To compute $2P = (x3, y3)$ we have $\lambda = 3x_2^2 1 + a 2y1 \equiv (3 \cdot 2^2 + 1)/(14) \equiv 13/14 \equiv 2/3 \equiv 2 \cdot 4 \equiv 8 \equiv \bmod 11$ Therefore $x3 = \lambda^2 - x1 - x2 \equiv 8^2 - 2 - 2 \equiv 60 \equiv 5 \bmod 11$ and $y3 = \lambda(x1 - x3) - y1 \equiv 8(2 - 5) - 7 \equiv -31 \equiv -9 \equiv 2 \bmod 11$ Use P and 2 P to prove that it is on same curve (6)	10 M
	OR	
2.	Properties of Hash Functions (2x5) 1. Non-reversibility, or one-way function. A good hash should make it very hard to reconstruct the original password from the output or hash. 2. Diffusion, or avalanche effect. A change in just one bit of the original password should result in change to half the bits of its hash. In other words, when a password is changed slightly, the output of enciphered text should change significantly and unpredictably. 3. Determinism. A given password must always generate the same hash value or enciphered text. 4. Collision resistance. It should be hard to find two different passwords that hash to the same enciphered text. 5. Non-predictable. The hash value should not be predictable from the password.	10 M

3.	**El-gamal algorithm (5)**
	Solving the given data (5)
	• use field GF(19) q=19 and a=10
	• Alice computes her key:
	  • A chooses x_A=5 & computes $y_A = 10^5 \bmod 19 = 3$
	• Bob send message m=17 as (11,5) by
	  • chosing random k=6
	  • computing $K = y_A^k \bmod q = 3^6 \bmod 19 = 7$
	  • computing $C_1 = a^k \bmod q = 10^6 \bmod 19 = 11$;
	$C_2 = KM \bmod q = 7.17 \bmod 19 = 5$
	• Alice recovers original message by computing:
	  • recover $K = C_1^{xA} \bmod q = 11^5 \bmod 19 = 7$
	  • compute inverse $K^{-1} = 7^{-1} = 11$
	  • recover $M = C_2 K^{-1} \bmod q = 5.11 \bmod 19 = 17$
		10 M

	OR	
4.	**HMAC working (8)** **Examples (2)**	10 M
5.	**Any five differences between Kerberos 5 and 4 (2x5)**	10 M

	OR	
6.	Working of Elgamal Schorr scheme (8) Example (2)	10 M
	PART B	
7.	PKI Mechanism (4) Design of PKI Certificate (6)	10 M
8.	IDS (6) Stages of IDS and Hash processing (4)	10 M

BMS INSTITUTE OF TECHNOLOGY AND MANAGEMENT

Avalahalli, Doddaballapur Main Road, Bengaluru - 560064

THIRD INTERNAL ASSESSMENT TEST, SEPT 2020 - 21

Name of the Course	Advanced Cryptography	Course Code	20SCS241
Branch & Semester	2nd Sem M.Tech CSE	Date	21-09-2021 (2:00PM-3:30PM)
Name of the Course Coordinator	Dr. Anjan Krishnamurthy	Max. Marks	50

Note: *Answer* ***THREE*** *full questions from* ***Part A*** *and* ***Part B*** *questions are compulsory.*

Qn. No.	PART A	Marks	CO
1.	Illustrate the working of Extranets with the help of diagram.	10 M	CO2, K3
	OR		
2.	Differentiate the working of packet filter and application gateway firewalls.	10 M	CO2, K4
3.	Illustrate the working of the Quantum one time pad cryptosystem.	10 M	CO4,K4
	OR		
4.	Analyze the performance metrics of various firewall types and suggest suitable firewall for educational institutions.	10 M	CO2, K4
5.	Write the different measurements used in Quantum machine. Compare how Qubit is different from classical bit system.	10 M	CO4, K4
	OR		
6.	Distinguish the various categories of the malicious software. Use diagram wherever required.	10 M	CO3, K4
	PART B		
7.	**Innovative question** Using the BB84 protocol, encrypt the message "Attack on the dawn". Indicate the states of the quantum particles using Hibert space.	10 M	CO4, K5
8.	**Case Study Question** In a satellite-based Quantum Key Distribution (QKD), highlight the important requirements to considered. Generate a sample QKD for this scenario using normal Bell states.	10 M	CO3, K5

Course Outcomes (COs)

CO1:	Apply the basic modular arithmetic concepts and set theory properties in cryptographic algorithms for encryption and decryption, hash functions, PRNGS. (K3)
CO2:	Identify suitable firewall and authentication mechanism for real time protection against any attacks. (K4)
CO3:	Evaluate the strength of cryptographic algorithms based on attack modeling and publish results.(K5)
CO4:	Develop exploratory study in analyzing the potential impact on futuristic development of cryptographic system in the areas of quantum cryptography, DNA cryptography. (K6)

Revised Bloom's Category

Remembering (K1) **Understanding (K2)** **Applying (K3)** **Analyzing (K4)** **Evaluating (K5)** **Creating (K6)**

Signatures of the Question Paper Scrutiny Committee

Course Coordinator(s)	Module Coordinator(s)	Program Coordinator	Head of the Department
17/9/2021	17/9/2021	17/9/2021	20/9/21

BMS INSTITUTE OF TECHNOLOGY AND MANAGEMENT

Avalahalli, Yelahanka, Doddaballapura Main Road, Bengaluru - 560064

THIRD ASSESSMENT TEST, Sept 2020 - 21

Name of the Course	**Advanced Cryptography**	**Course Code**	**20SCS241**
Branch & Semester	**2nd Sem M.Tech CSE**	**Date**	**21-09-2021 (2:00PM-3:30PM)**
Name of the Course Coordinator	**Dr. Anjan Krishnamurthy**	**Max. Marks**	**50**

Scheme and Solution

Qn. No.	PART A	Marks
1.	Diagram (3) Extranets Working (7m)	10 M
	OR	
2.	Any five differences between Packet filtering and Application gateway (2x5)	10 M
3.	Quantum systems (4) One time pad (6)	10 M
	OR	
4.	Parameter definition (Speed, Flexibility, Intelligence) – 6m Explanation (4m)	10 M
5.	Diagram (2 m) Differences between various categories with support of host and no host (2x4)	10 M
	OR	
6.	Measurements in Quantum Machine (6m) Qubit Vs Binary Bit (4m)	10 M
	PART B	
7.	BB84 protocol (6m) Encryption (4m)	10 M
8.	QKD (6m) Sample of QKD (4m)	10 M

BMS INSTITUTE OF TECHNOLOGY AND MANAGEMENT

YELAHANKA, BENGALURU – 560064

Department of Computer Science and Engineering

Date: 25th Jun 2021

Course Name: Advanced Cryptography **Faculty:** Dr. Anjan Krishnamurthy

Type of Assignment: Literature Survey with implementation of Cryptographic Algorithms

Assignment list for AC 20SCS241 – 2020-21

Sl. No.	USN	Student Name	Topic Name	RBT	CO	PO1	PO2	PO3	PO4	PO5	PO6
1.	1BY20SCS01	Adithya Sharma B S	ECC - El Gamal	K4	CO4	√	√				√
2.	1BY20SCS02	Arunkumar K Bhavikatti	ECC -Paillier cryptosystem	K4	CO4	√	√				√
3.	1BY20SCS03	Bhavana G V	ECC - Rabin	K4	CO4	√	√				√
4.	1BY20SCS04	CHERUKU YASASWINI	ECC -Cayley–Purser algorithm	K4	CO4	√	√				√
5.	1BY20SCS05	Pragna M V	ECC -Benaloh cryptosystem	K4	CO4	√	√				√
6.	1BY20SCS06	Priyanka	ECC - Merkle–Hellman	K4	CO4	√	√				√
7.	1BY20SCS08	SRIDHAR H S	ECC -Schmidt-Samoa cryptosystem	K4	CO4	√	√				√
8.	1BY20SCS09	Tejaswini Halakate	ECC -McEliece cryptosystem	K4	CO4	√	√				√
9.	1BY20SCS10	Umme Aymun	ECC -Goldwasser–Micali	K4	CO4	√	√				√

BMS INSTITUTE OF TECHNOLOGY AND MANAGEMENT

YELAHANKA, BENGALURU – 560064

Department of Computer Science and Engineering

Rubrics

Dimension	Maximum Marks	High	Medium	Low
Introduction		Position and exceptions, if any, are clearly stated. Organization of the argument is completely and clearly outlined and implemented.	Position is clearly stated. Organization of argument is clear in parts or only partially described and mostly implemented.	Position is vague. Organization of argument is missing, vague, or not consistently maintained.
	5	4-5 pts	2-3 pts	0-1 pts
Research		Research selected is highly relevant to the argument, is presented accurately and completely – the method, results, and implications are all presented accurately; Theory is relevant, accurately described and all relevant components are included; relationship between research and theory is clearly articulated and accurate.	Research is relevant to the argument and is mostly accurate and complete – there are some unclear components or some minor errors in the method, results or implications. Theory is relevant and accurately described, some components may not be present or are unclear. Connection to theory is mostly clear and complete, or has some minor errors.	Research selected is not relevant to the argument or is vague and incomplete – components are missing or inaccurate or unclear. Theory is not relevant or only relevant for some aspects; theory is not clearly articulated and/or has incorrect or incomplete components. Relationship between theory and research is unclear or inaccurate, major errors in the logic are present.
	5	4-5 pts	2-3 pts	0-1 pts
Conclusions		Conclusion is clearly stated and connections to the research and position are clear and relevant. The underlying logic is explicit. 4-5 pts	Conclusion is clearly stated and connections to research and position are mostly clear, some aspects may not be connected or minor errors in logic are present.	Conclusion may not be clear and the connections to the research are incorrect or unclear or just a repetition of the findings without explanation.

				Underlying logic has major flaws; connection to position is not clear.
	5	**4-5 pts**	**2-3 pts**	**0-1**
Report Writing		Paper is coherently organized and the logic is easy to follow. There are no spelling or grammatical errors and terminology is clearly defined. Writing is clear and concise and persuasive.	Paper is generally well organized and most of the argument is easy to follow. There are only a few minor spelling or grammatical errors, or terms are not clearly defined. Writing is mostly clear but may lack conciseness.	Paper is poorly organized and difficult to read – does not flow logically from one part to another. There are several spelling and/or grammatical errors; technical terms may not be defined or are poorly defined. Writing lacks clarity and conciseness.
	5	**4-5 pts**	**2-3 pts**	**0-1**

Grading policies:

- The last date for the submission of the assignment is on or before **6th Sept 2021 (hard deadline).**
- The assignment must be unique contribution and will undergo rigorous plagiarism process. This similarity index must be less than or equal to 25%.
- The report of the assignment must detail out in 2-column IEEE paper format.
- Care to be taken for representation of facts, diagrams, grammar.
- The assignment can be simple prototype implement, deeper exploration of technology, novel thoughts, and ideas on the topics.
- A 15-20 slides ppt must be presented within 5 working days from the submission date. **(11th Sept 2021)**

Grading will be based on punctual submission of the assignment.

Feed Back and Analysis:

- Students have implemented real time crypto algorithms with respect to Advanced Cryptography domain. The implementation helped them to learn new concept enabling research work in this domain. Through this assignment students are enabled to attain CO4, PO1, PO2 and PO6.

Course Coordinator Signature:

REFERENCES

(As per IEEE format and must be numbered consecutively in order of first mention)

Example format:

Journal Paper: Name initial, —titleǁ, Journal name, vol. **(issue), year, pp.11

1. Honig, M.L., Steiglitz, K., and Gopinath, B., —Multichannel signal processing for data communication in the presence of crosstalkǁ, *IEEE Trans. Communications.*, vol. 38, (4), 1990 , pp. 551–558.

Conference Proceedings: Name Initial, —titleǁ, Proceeding of the *, place, year, pp. ***

2. Shin, K.G. and Mckay, N.D. —Open Loop Minimum Time Control of Mechanical Manipulations and its Applicationsǁ *Proceedings of the Amer. Contr. Conf., San Diego, CA, ,1984,* pp. 1231-1236

Patent: Name initial, —title of patentǁ, Patent number, date of patent

3. Bischoff F, —Apparatus for vapor deposition of silicon,ǁ U.S. *Patent* 3 335 697, Aug. 15, 1967

Thesis (Masters / Doctoral): Name, initials, —titleǁ, University, Year

1. Nongpiur, R C, —Near-End Crosstalk Cancellation in xDSL Systemsǁ *Doctoral thesis, University of Victoria*, 2005

Annual reports / manual: Name (optional), —titleǁ, Report number, Agencies, Year

5. The International Technology Roadmap for Semiconductors, Report-7, ITRS, 2011,

Books / Manual / standards data hand books: —Title —, publisher, year

6. —Ferrous Material Testing Procedure — ASTM Standard- vol.3, American Society for Testing Materials, 2003

BMS Institute of Technology and Management

Department of Computer Science & Engineering

IA Marks Details for the Even Semester 2020-21

Sem: 2nd Sem M.Tech CSE Course Name with code: AC (20SCS241) Name of Faculty: Dr. Anjan Krishnamurthy

Sl. No.	NAME	USN	Test1	Test2	Test3	Avg	Rounded	Assignment	Final
1	Adithya Sharma B S	1BY20SCS01	19	18	17	18.5	19	11	30
2	Arunkumar K Bhavikatti	1BY20SCS02	11	18	18	18	18	10	28
3	Bhavana G V	1BY20SCS03	20	19	16	19.5	20	15	35
4	CHERUKU YASASWINI	1BY20SCS04	19	18	16	18.5	19	14	33
5	Pragna M V	1BY20SCS05	20	18	18	19	19	16	35
6	Priyanka	1BY20SCS06	19	18	16	18.5	19	15	34
7	SRIDHAR H S	1BY20SCS08	13	12	12	12.5	13	12	25
8	Tejaswini Halakate	1BY20SCS09	20	17	13	18.5	19	18	37
9	Umme Aymun	1BY20SCS10	20	18	18	19	19	15	34